

Invitation to Attend:

The NIST Federal Government Workshop on *Applying FIPS 199 and SP 800-60 to Industrial Control Systems (ICS)*.

September 5-6, 2007

NIST

Administration Building, Lecture Room E

Gaithersburg, MD 20899

The National Institute of Standards & Technology (NIST) will host a workshop for federal agencies that own or operate industrial control system (ICS) to discuss the application of FIPS 199: *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, to ICS. The goal of this workshop is to develop guidance (technical and non-technical) that federal agencies can use in applying FIPS 199 to their ICS.

Background:

At previous workshops on applying NIST's FISMA-related documents to ICS (e.g., FIPS 200, NIST SP 800-53), federal agencies that own or operate ICS indicated they had difficulty in determining the security categorization of ICS, particularly when they had to take into account the impact to their organization, dependent organizations, and critical infrastructures. They pointed out that guidance for determining impact was lacking and that other related factors/considerations had to be identified/discussed such as:

- Resolution of different view points from within (e.g., system owners, internal auditors, IGs) and without (e.g., external auditors) the organization
- Boundary problems including interconnectivity, complexity, interdependence, redundancy
- The relationship between ICS system architectures & ICS security controls. As examples:
 - When performing security categorization of an ICS that operates in an environment containing other backup/redundant ICS, is the redundancy treated as a control—in which case it is ignored when making a worst case FIPS 199 categorization decision-- or should the redundancy be taken into consideration when performing the security categorization?
 - How is a system-of-systems treated?
 - How are sub-systems with multiple ownership treated?

To address these issues, the federal agencies strongly recommended NIST hold a security categorization workshop that:

- Shares the experiences of the federal agencies in attempting to apply FIPS 199 to ICS and identifies/discusses the concerns raised by federal agencies in their attempts to apply FIPS 199
- Addresses tailoring the FIPS 199 security categorization process for ICS

- Provides guidance that can be incorporated into a revised version of NIST SP 800-60: *Guide for Mapping Types of Information and Information Systems to Security Categories*,
- Provides guidance in addressing architectural and other technical issues; and non-technical issues.

This workshop is a result of the federal agencies' recommendations.

If you are interested in attending the workshop, please send email to:

Stu Katzke at: skatzke@nist.gov or Keith Stouffer at: keith.stouffer@nist.gov.

PLEASE NOTE:

1. Attendance at the workshop is restricted to federal agencies (including IT and ICS subject matter experts) and/or their contractors. In addition, federal agencies are strongly encouraged to invite representatives from their internal audit and IG communities to attend the workshop. All non-federal government attendees must be nominated and accompanied by their federal agency client/sponsor.
2. Attendance at the workshop requires that a completed questionnaire be submitted from each attendee to NIST by August 17, 2007. When submitting the questionnaire, attendees should use the input form that will be posted on the NIST FISMA ICS webpage (<http://csrc.nist.gov/sec-cert/ics>). After receiving the questionnaires, NIST will develop and distribute, at the workshop if not before, a synthesis to be used as a starting point for workshop discussions.